PARLEU2017.EE

Parliamentary Dimension
of the Estonian Presidency
of the Council of the
European Union

Conférence interparlementaire sur la politique étrangère et de sécurité commune (PESC) et sur la politique de sécurité et de défense commune (PSDC)
7-9 septembre 2017, Tallinn

Informations de base

Aspects pratiques du monde hybride, notamment le domaine cybernétique et la communication stratégique

Le monde contemporain repose de plus en plus sur les technologies numériques, qui le rendent vulnérable aux cybermenaces. En même temps, des moyens hybrides sont utilisés, à la place des instruments conventionnels, pour faire pression sur les États souverains. Les menaces hybrides ont été définies comme *un mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles (c'est-à-dire diplomatiques, militaires, économiques, technologiques), susceptibles d'être utilisées de façon coordonnée par des acteurs étatiques ou non étatiques en vue d'atteindre certains objectifs, sans que le seuil d'une guerre déclarée officiellement ne soit dépassé*.[1]

L'UE a pris plusieurs mesures pour cibler les menaces hybrides et les cybermenaces.

Actions de l'UE visant à combattre les menaces hybrides et les cybermenaces

La stratégie de cybersécurité de l'UE, publiée en 2013, détermine les cinq domaines prioritaires pour un cyberespace européen plus sécurisé, parmi lesquels figurent l'élaboration d'une politique de cyberdéfense et le développement des capacités relevant de la politique de sécurité et de défense commune de l'UE (PSDC). L'UE œuvre à élaborer une nouvelle stratégie de cybersécurité.

Le 6 avril 2016, la Commission a publié une communication adressée conjointement au Parlement européen et au Conseil (cadre commun en matière de lutte contre les menaces hybrides). 22 actions ont été proposées pour lutter contre les menaces hybrides, pour renforcer la résilience et pour améliorer la coopération entre tous les acteurs concernés, tout en complétant les autres politiques et les documents déjà existants: le programme européen en matière de sécurité, la stratégie globale pour la politique étrangère et de sécurité de l'Union européenne et le plan d'action européen de la défense, la stratégie de cybersécurité de l'UE, la stratégie européenne pour la sécurité énergétique et la stratégie de sûreté maritime de l'Union européenne. Le 19 juillet 2017, la Commission a publié un rapport sur la mise en œuvre du cadre commun en matière de lutte contre les menaces hybrides, faisant état des progrès significatifs accomplis dans les 22 actions proposées. En juillet 2016, le protocole opérationnel de l'UE de lutte contre les menaces hybrides (EU Playbook) a été adopté. Ce document précise les modalités pratiques de coordination, de fusion et d'analyse des renseignements et de coopération avec l'OTAN. En 2016, une cellule de fusion de l'UE contre les menaces hybrides a été établie au sein du Service européen pour l'action extérieure, afin de fournir des analyses des données de toutes sources sur les menaces hybrides.

[1] JOIN (2016) 18 final

Les task forces StratCom

À l'ère de la post-vérité, des faits alternatifs et de l'excès d'informations, il est extrêmement important de distinguer les informations et les faits exacts des informations destinées à détourner l'attention des décideurs politiques et du public. Cela a conduit à la création des task forces contre la désinformation. Si la task force East StratCom s'occupe des campagnes de désinformation de la Russie, la task force Arab StratCom lutte contre la radicalisation dans le monde arabe.

Coopération OTAN-UE sur les cybermenaces et les menaces hybrids

La déclaration commune sur la coopération OTAN-UE a été signée par les dirigeants de l'UE et le secrétaire général de l'OTAN en juillet 2016. Elle a été suivie de 42 propositions concrètes en décembre 2016. La cybersécurité ainsi que la lutte contre les menaces hybrides sont parmi les priorités des propositions. Le premier rapport sur l'état d'avancement, indiquant que des efforts considérables ont été accomplis (notamment dans le domaine cybernétique), a été publié en juin 2017. Un nouvel élargissement de la coopération sera probablement envisagé dans le prochain rapport, qui devra être soumis en décembre.

Autres initiatives

En outre, les États membres et l'OTAN ont également pris d'autres initiatives:

Plusieurs centres de recherche ont été établis afin de combattre les menaces hybrides et les cybermenaces. L'un d'entre eux, le Centre d'excellence européen pour la lutte contre les menaces hybrides, a été fondé en avril 2017. Son objectif est de sensibiliser le public aux menaces hybrides et aux vulnérabilités des sociétés qui sont susceptibles d'être exploitées lors des opérations hybrides, et de favoriser la résilience des sociétés. Les deux autres centres de recherche, à savoir le Centre d'excellence pour la communication stratégique de l'OTAN en Lettonie et le Centre d'excellence pour la cyberdéfense coopérative de l'OTAN en Estonie, combattent les menaces similaires concernant le domaine cybernétique, les menaces hybrides et la communication stratégique.

Le Centre d'excellence pour la cyberdéfense coopérative de l'OTAN a dirigé le processus de rédaction et de publication du Manuel de Tallinn 2.0 (une version mise à jour du Manuel de Tallinn de 2013) en 2017, qui se penche sur l'applicabilité du droit international aux cyberopérations.

Points de discussion

1. Comment renforcer la résilience contre les cyberattaques dans le monde en évolution rapide des technologies?
2. Les cybermenaces sont-elles un phénomène nouveau?
3. Comment développer chez les citoyens un sens de la responsabilité et une pensée critique vis-à-vis de la consommation des médias?